

Exhibit A

DECLARATION OF ROMAN BIEDA

I DECLARE under penalty of perjury that the following is true and correct:

1. My name is Roman Bieda. I am over 18 years of age. I have personal knowledge of the matters set forth herein.

2. Since December 2023, I have been the Head of Investigations for Token Recovery. Prior to joining Token Recovery, I was the Head of Fraud Investigations of Coinfirm Ltd. (“Coinfirm”).

3. I have reviewed the Declaration of Bruno Requiao da Cunha and his criticism of Coinfirm’s investigation and my declarations dated December 27, 2022 and December 30, 2022. Before I address the substance of his criticism, there are a number of issues with Mr. Cunha’s Declaration that need to be addressed.

Issues with Mr. Cunha’s Declaration

4. Mr. Cunha claims to hold a number of blockchain, digital forensics and investigative certificates. *See* Declaration of Bruno Requiao Da Cunha (“Cunha Dec.”), at ¶2. However, Mr. Cunha omits that seven of the eight certificates listed were issued by his employer, TRM Labs, as opposed to having been issued by an independent certification organization. The only certificate not issued by TRM Labs relates to a \$300 online course instructing people on the use of Solidity—an object-oriented programming language—to build and deploy smart contracts on Ethereum. *See* <https://www.blockchain-council.org/certifications/certified-solidity-developer/>. The Solidity Developer certification—learning how to use Solidity’s language to program Ethereum smart contracts—does not qualify a person to perform forensic blockchain investigations.

5. Mr. Cunha also omits that one of the services TRM Labs offers its customers is to have its experts manually trace Bitcoin through mixers that perform the same function as ChipMixer. Ironically, Mr. Cunha even indicates that his position as a Global Investigator for TRM Labs, includes investigation of complex cases “using a combination of advanced investigative tactics such as *demixing and complex tracing*.” See Cunha Dec., at ¶2 (emphasis added). Thus, when Mr. Cunha claims that “privacy features made ‘Bitcoin tracing nearly impossible after mixing funds through ChipMixer,’” he is either dramatically overstating the “impossibility” of tracing Bitcoin through ChipMixer or is casting significant doubt over TRM Labs’ claims of being able to trace Bitcoin through cryptocurrency mixers.

6. Mr. Cunha’s statements regarding ChipMixer itself are also inaccurate. Specifically, Mr. Cunha states that ChipMixer is based in Hanoi, Vietnam. However, those more familiar with ChipMixer know that it was not explicitly based in Vietnam. The service operated primarily online, making it difficult to pinpoint a specific physical location or “base” for its operations. Multiple authorities and media outlets have reported that one of the individuals allegedly involved with ChipMixer, a person named Hoang, was arrested in Vietnam in connection with the platform’s activities, and the U.S. Department of Justice charged Minh Quoc Nguyen of Hanoi, Vietnam with various crimes in connection with ChipMixer. However, ChipMixer’s servers were based in a former NATO bunker in Traven-Trarbach, Germany that had been repurposed into a data center. One of the Department of Justice press releases to which Mr. Cunha refers indicates that German law enforcement were involved in ChipMixer’s shutdown, and that German police seized “the ChipMixer back-end servers and more than \$46 million in cryptocurrency.” See Press Release, U.S. Department of Justice, Office of Public Affairs, *Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed*

Over \$3 Billion of Unlawful Transactions (Mar. 15, 2023), <https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3>. For someone who claims to be knowledgeable in “demixing and complex tracing,” Mr. Cunha’s incorrect statements regarding ChipMixer are surprising.

7. Mr. Cunha also omits the details of his and/or TRM Labs’ findings regarding the portion of the 11,825.148419 Bitcoin stolen from Cryptsy (the “Stolen Bitcoin”) and ultimately transferred out of ChipMixer to Ren.¹ When discussing his “independent blockchain review” of the Stolen Bitcoin, *see* Cunha Dec., ¶7, Mr. Cunha actually confirms my analysis and concludes, like I did, that the Stolen Bitcoin was transferred to ChipMixer. However, having confirmed that part of my analysis was correct, Mr. Cunha intentionally omits TRM Labs’ findings regarding the Stolen Bitcoin transferred out of ChipMixer and into Ren. If Mr. Cunha sincerely believes that Coinfirm utilized an improper approach to tracing Bitcoin through ChipMixer, then Mr. Cunha should have explained what he believes to be the proper methodology for such tracing. Likewise, if Mr. Cunha believes he and TRM Labs use “a combination of advanced investigative tactics such as demixing and complex tracing,” *see* Cunha Dec., at ¶12, through mixers, Mr. Cunha should have detailed the findings that he and TRM Labs made regarding the amount of Stolen bitcoin that went through ChipMixer and to Ren. I have no doubt that if Mr. Cunha performed the investigation that he claims to have performed, he would have determined that some amount of the Stolen Bitcoin went through ChipMixer and to Ren.

¹ Ren was responsible for the Ren Protocol, a decentralized blockchain protocol intended to facilitate interoperability between different blockchain networks, and allowing for the transfer of digital assets across various blockchains without relying on centralized intermediaries. This was implemented in Ren’s service, RenBridge, which allowed users to lock a digital asset on one network, e.g., BTC, to a digital asset on another network, e.g., Ethereum, thus allowing digital assets to move seamlessly across different blockchain networks. Due to its non-custodial nature, RenBridge was often used by bad actors, including those who stole \$477 million from FTX in November 2022.

Coinfirm's Investigation

8. From July, 2020 to December, 2023, I was the Head of Fraud Investigations of Coinfirm. As the Head of Fraud Investigations, I oversaw Coinfirm's Asset Tracking and Fraud Investigation tools and I led Coinfirm's Asset Tracking & Investigations Team on thousands of blockchain investigations.

9. As Coinfirm's Head of Fraud Investigations, I also had access to Coinfirm's tools utilized to track and trace BTC, including a tool that Coinfirm licenses on a Software-as-a-Service basis to certain forensic companies and law enforcement agencies in Europe. Some of these tools were tracking transactions in real-time, as opposed to trying to reconstruct transactions long after the transactions occurred.

10. When I was with Coinfirm, I also had access to the full investigatory file created in connection with the Stolen Bitcoin. This file included Coinfirm's real-time tracking of the Stolen Bitcoin. Had Mr. Cunha come forward with his criticism of Coinfirm's investigation and tracing of the Cryptsy Stolen Bitcoin through ChipMixer and to Ren around the time that I signed my December 27, 2022 declaration, I would have been able to utilize Coinfirm's complete investigatory file, and the precise tracking data that Coinfirm had assembled, when addressing Mr. Cunha's criticism. I had no right to take Coinfirm's investigatory file regarding the Cryptsy Stolen Bitcoin with me when I left Coinfirm, and I do not presently have access to Coinfirm's file. However, a number of Mr. Cunha's criticism are so lacking in merit that I am able to respond to his criticism with what I still recall from Coinfirm's investigation and based on publicly available information.

Mr. Cunha's Unwarranted Criticism of Coinfirm's Investigation

11. First, Mr. Cunha claims that I did not explain how any of the Stolen Bitcoin was traced to Ren, and that “it is not possible to conclude with any confidence that the BTC that [I] identifie[d] as having been transferred to RenBridge . . . are the same BTC that was stolen from Cryptsy....” *See* Cunha Dec., ¶¶ 11-12. Coinfirm’s tool tracked the Stolen Bitcoin through ChipMixer and to Ren, and that is precisely what I detailed in my prior declarations. While Coinfirm’s methodology did not establish that the same person was involved on either end of the transaction, the tracing that Coinfirm performed did follow the Stolen Bitcoin. It is a common strategy for investigators to trace BTC up to the first identifiable cryptocurrency service—for example, Coinbase—that can either freeze the traced BTC or provide the know your customer (“KYC”) information for the person who received tainted BTC and deposited it into the identifiable service. In this instance, the Stolen Bitcoin could only have been transferred to ChipMixer by Paul Vernon—Cryptsy’s former CEO—or someone who obtained the keys necessary to effectuate the transfer to ChipMixer from Mr. Vernon. Thus, transactions were followed from the wallet addresses listed in Table 1 and Table 2 in the Amended Final Judgment Against Defendant Paul Vernon (the “Amended Final Judgment”) to ChipMixer and then to the next identifiable service, which in this case was Ren.

12. Second, Mr. Cunha claims that I provided no explanation as to how Coinfirm’s primary tracing methodology, the Pro Rata Distribution by All Outputs methodology, works. However, companies like Coinfirm, TRM Labs, and Chainalysis that perform demixing and complex tracing do not typically disclose or even provide an explanation as to the precise algorithms and methodologies they use when performing such investigations. Instead, as Mr. Cunha almost certainly knows, each of the companies claim that the details of their algorithms

and methodology are proprietary and confidential, and they do not disclose such information even to their customers (as far as I am aware, TRM never provides an explanation of its tracing and clustering methodologies in its reports, instead claiming that such information is proprietary). If Mr. Cunha is not willing to disclose what he believes the proper methodology is, and not willing to disclose the details of TRM Labs' methodologies, any criticism regarding Coinfirm's desire to maintain confidentiality over the same, closely-guarded information that TRM Labs deems to be highly confidential, is improper.

13. Third, Mr. Cunha presents an example of how mixing services work. *See* Cunha Dec., ¶14. He even correctly observes that “a proportional allocation method would inaccurately dilute the percentage of funds belonging to a particular user across multiple transactions and users....” *See* Cunha Dec., ¶15. The example that Mr. Cunha presents, and his observation regarding proportional allocation, is the way that ChipMixer was, in theory, intended to operate. However, Mr. Cunha fails to acknowledge that when larger amounts of BTC are mixed through ChipMixer with no other change in the number of users or transactions, ChipMixer's ability to “dilute the percentage of funds belonging to a particular user across multiple transactions and users” is severely impaired. Ultimately, the flood of Stolen Bitcoin—an amount of BTC many times greater than the total pool of BTC that ChipMixer had at the time—caused ChipMixer's theoretical approach to break down because it could not handle the Stolen Bitcoin and achieve proportional allocation.

14. To better understand why ChipMixer could not provide adequate anonymity for Stolen Bitcoin deposits, consider the following variation on Mr. Cunha's example. If you think of ChipMixer as a box, and instead of BTC, imagine that ChipMixer users are placing dollar bills into the box. If the total pool contains 600 dollar bills, and each of users A, B and C contribute

roughly similar amounts (e.g., 100, 200 and 300 dollar bills as Mr. Cunha used), then the proportionality lowers the probability that each of A, B and C will receive the same dollar bills that they originally put into the box. However, if those figures are skewed by one participant contributing a significant majority of dollar bills—perhaps 550 of the 600 placed in the box—and the other users each contribute 25, the probability that the large contributor received his or her own dollar bills increases significantly.

15. In reality, Mr. Vernon (or someone working with him to whom Mr. Vernon provided the keys necessary to transfer the Stolen Bitcoin) flooded ChipMixer with such a large amount of BTC in such a short period of time that it effectively impaired ChipMixer's ability to achieve proportionality.

16. Prior to Mr. Vernon flooding ChipMixer with the Stolen Bitcoin, ChipMixer's Bitcoin pool—the amount of Bitcoin that ChipMixer maintained daily—was roughly 2,000 BTC. Beginning in March, 2022, when Mr. Vernon started transferring the bulk of the Stolen Bitcoin into ChipMixer, ChipMixer's total BTC pool jumped from roughly 2,000 BTC to close to 14,000 BTC. Over the course of the next few weeks, as ChipMixer transferred the Stolen Bitcoin back to accounts where Vernon wanted it sent, ChipMixer's total pool of BTC started to decline as the Stolen Bitcoin was transferred out to various places, including Ren. By the end of April, 2022, ChipMixer's total BTC pool had dropped to roughly 6,000 BTC, still three times higher than where it started prior to ChipMixer receiving the Stolen Bitcoin. This dramatic set of changes can be seen in Figure 1 below:

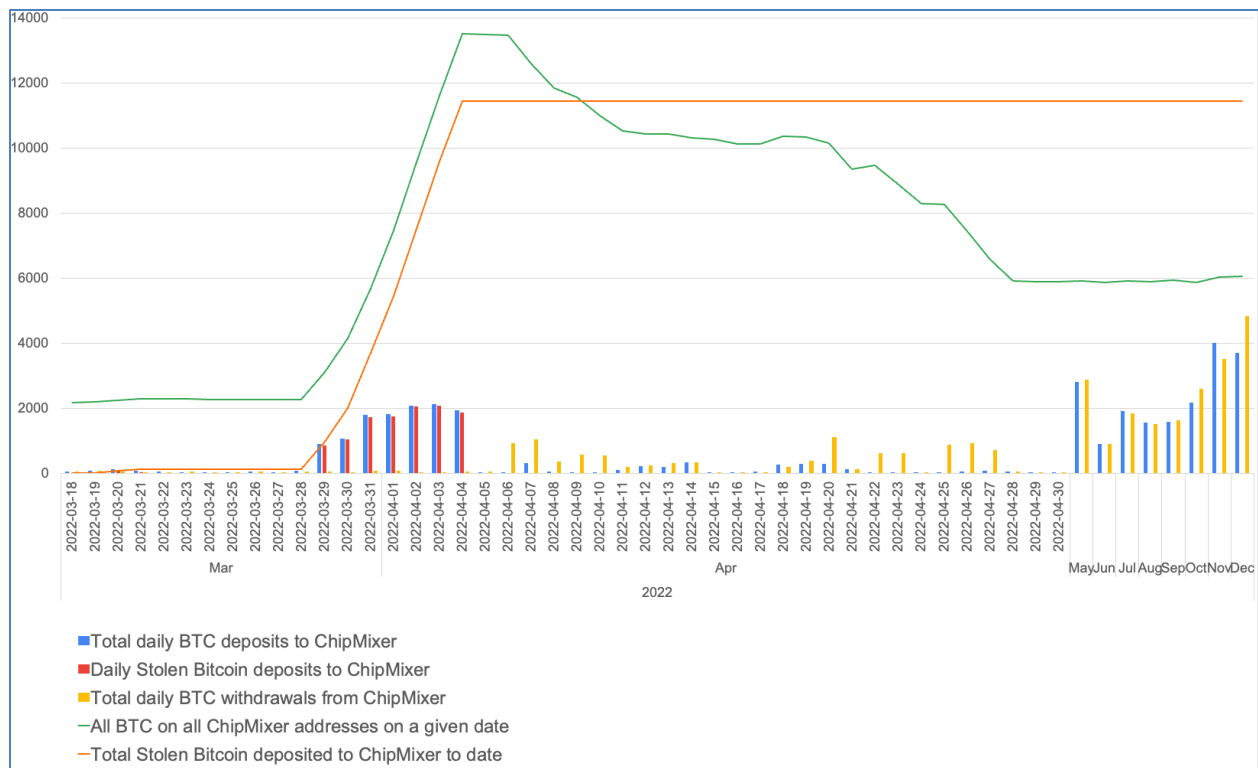


Figure 1 - ChipMixer Pool Volume

17. Thus, the amount of Stolen Bitcoin run through ChipMixer was so much greater than the amounts ordinarily deposited and withdrawn from ChipMixer that ChipMixer’s ability to “dilute the percentage of funds” was dramatically reduced. As a result, a variety of approaches were available to ascertain with a reasonable likelihood of probability, that the BTC leaving ChipMixer was, in fact, the Stolen Bitcoin that Mr. Vernon had transferred into ChipMixer.

18. Mr. Cunha also takes issue with the various other tracing methodologies that Coinfirm used. For instance, Mr. Cunha criticizes what I termed the “First in First Out” and “Last in First Out” methodologies based on an assumption that these are “accounting conventions that...have the same flaws as a proportional attribution method and cannot be used effectively to de-mix crypto transactions....” *See Cunha Dec.*, ¶17. However, this criticism ignores the impact of Mr. Vernon flooding ChipMixer with the Stolen Bitcoin, and destroying ChipMixer’s ability to achieve any meaningful proportionality. Additionally, Mr. Cunha fails to realize that each of the

various methodologies factored into Coinfirm's analysis, the precise details of which are proprietary and confidential to Coinfirm. That said, it is apparent that Mr. Cunha's criticism of the methods referenced in my Declaration are based on a fundamental misunderstanding as to the role each of those methods plays in the analysis.

19. As indicated in my Declaration, Coinfirm employed a methodology referred to as "Pro Rata Distribution by All Outputs," supported by four additional methodologies. The precise details of how Coinfirm utilizes these methodologies with its proprietary tracking tools is confidential. However, without disclosing aspects of the methodology confidential to Coinfirm, I can generally explain each of the various forensic accounting approaches identified in my Declarations.

20. Digital asset tracking involves identifying and evidencing the destination or source of digital assets through the application of various forensic accounting methods. Digital assets resulting from illicit activity are typically passed through complex layering/mixing schemes aimed at concealing the trail of funds.

21. Each digital asset tracking exercise starts with the provision of transfers to be traced. Unlike in traditional finance, blockchain transactions may contain several transfers of funds occurring in one transaction, where only part of them should be subject to tracing. Therefore, tracking should always be executed on the lowest level of granularity which is a transfer and not a transaction, address, or cluster.

22. With these goals in mind, the following forensic accounting methodologies are often utilized in the course of investigating the movement of tainted digital assets:

- Pro Rata Distribution by All Outputs: Also referred to as the "Haircut" method, this is a transaction tracking method based on the relative percentages of tainted

and untainted digital assets that are allocated to subsequent transactions. The term “by All Outputs” indicates that it is a variation of the Pro Rata Distribution method, which iteratively propagates taint through all outgoing transactions known for the time of analysis, appearing after each consecutive block (iteration of transaction tracking algorithm). This approach also takes into account the timing of various transactions. Figure 2 below illustrates this method and some of the rules applicable to the method.

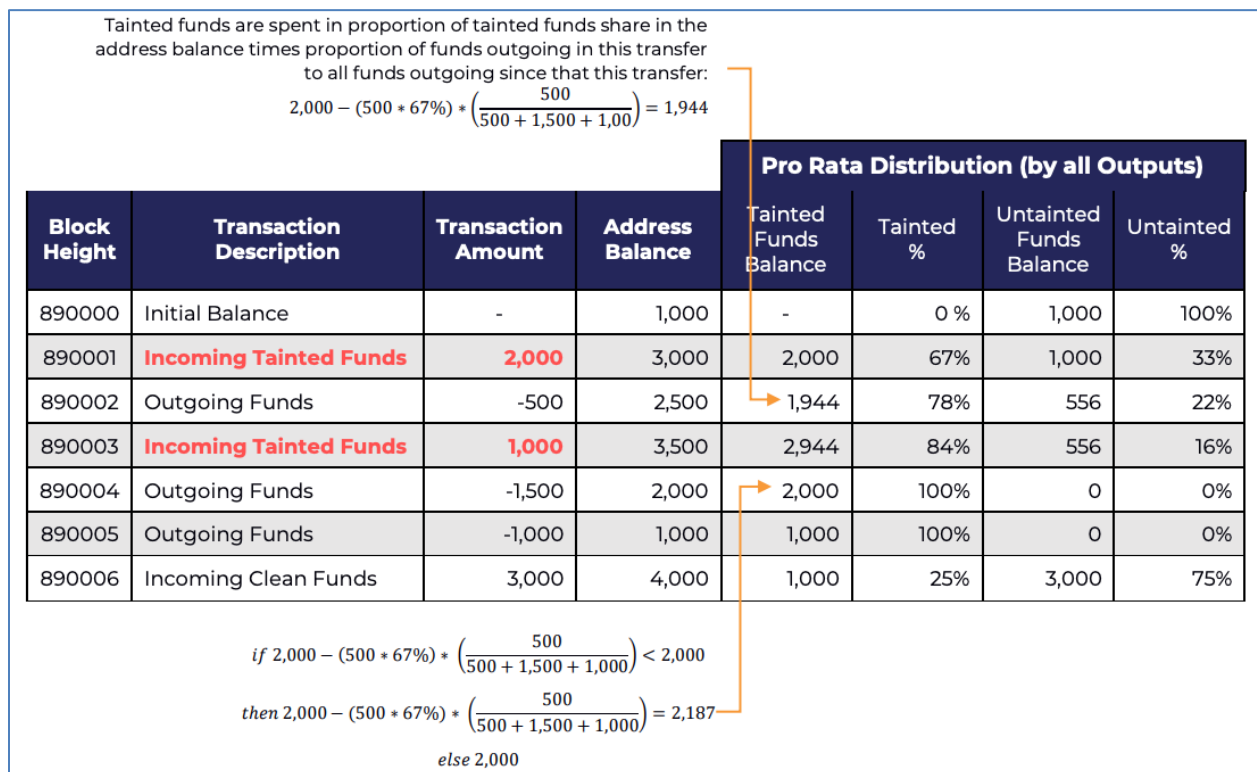


Figure 2. Example of Pro Rata Distribution by All Outputs

- First In First Out (“FIFO”): This is a transaction tracking method based on the established order of the transactions. If tainted digital assets are sent to an address that already contained non-tainted digital assets, the non-tainted and tainted digital assets will leave the account in the same order as received. Figure 3 below

illustrates this approach. As Mr. Cunha confirms, this tracing method is often used in financial investigations. *See* Cunha Dec., ¶17.

Block Height	Transaction Description	Transaction Amount	Address Balance	First In First Out (FiFo)	
				Tainted Funds Balance	Untainted Funds Balance
890000	Initial Balance	-	1,000	-	1,000
890001	Incoming Tainted Funds	2,000	3,000	2,000	1,000
890002	Outgoing Funds	-500	2,500	2,000	500
890003	Incoming Tainted Funds	1,000	3,500	3,000	500
890004	Outgoing Funds	-1,500	2,000	2,000	0
890005	Outgoing Funds	-1,000	1,000	1,000	0
890006	Incoming Clean Funds	3,000	4,000	1,000	3,000

Untainted funds were first on the balance, therefore tainted funds are spent first
 $(1,000 - 500) = 500$

Figure 3. Example of FIFO

- Last In First Out (“LIFO”): This is another transaction tracking method based on the order of the transactions, but unlike FIFO, the most recently received digital assets, regardless of whether they are tainted, are treated as the first to be sent out in a subsequent transaction. Figure 5 below illustrates this approach.

Block Height	Transaction Description	Transaction Amount	Address Balance	Last In First Out (LiFo)	
				Tainted Funds Balance	Untainted Funds Balance
890000	Initial Balance	-	1,000	-	1,000
890001	Incoming Tainted Funds	2,000	3,000	2,000	1,000
890002	Outgoing Funds	-500	2,500	1,500	1,000
890003	Incoming Tainted Funds	1,000	3,500	2,500	1,000
890004	Outgoing Funds	-1,500	2,000	1,000	1,000
890005	Outgoing Funds	-1,000	1,000	0	1,000
890006	Incoming Clean Funds	3,000	4,000	0	4,000

Tainted funds were received last, therefore tainted funds are spent first
 $(2,000 - 500) = 1,500$

Figure 4. Example of LIFO approach

Like FIFO, Mr. Cunha confirms that LIFO is also a tracing method often used in financial investigations. *See Cunha Dec.*, ¶17.

- “Pro Rata Distribution by Blocks:” This method considers the relative percentages of tainted and untainted funds that are allocated to subsequent transactions. The term ‘by Block’ indicates that it is a variation of the Pro Rata Distribution method, which iteratively propagates taint only through outgoing transactions appearing in specific consecutive blocks. In other words, each outgoing transaction includes both tainted and untainted digital assets in proportion. Figure 6 below illustrates this approach.

Block Height	Transaction Description	Transaction Amount	Address Balance	Pro Rata Distribution (by Block)			
				Tainted Funds Balance	Tainted %	Untainted Funds Balance	Untainted %
890000	Initial Balance	-	1,000	-	0 %	1,000	100%
890001	Incoming Tainted Funds	2,000	3,000	2,000	67%	1,000	33%
890002	Outgoing Funds	-500	2,500	1,667	67%	833	33%
890003	Incoming Tainted Funds	1,000	3,500	2,677	76%	833	24%
890004	Outgoing Funds	-1,500	2,000	1,524	76%	476	24%
890005	Outgoing Funds	-1,000	1,000	762	76%	238	24%
890006	Incoming Clean Funds	3,000	4,000	762	19%	3,238	81%

Tainted funds are spent in proportion of tainted funds share in the address balance:
 $2,000 - (500 * 67\%) = 1,667$

Figure 5. Example of Pro Rata Distribution by Blocks

- “Taint Last:” This is a method based on the established order of the transactions where untainted digital assets are presumed transacted before tainted digital assets. If an incoming transaction involves both tainted and untainted digital assets, the subsequent outgoing transaction will first use untainted digital assets. Figure 7 below illustrates this approach.

Untainted funds are always taken out first from the balance:
 $1,000 - 500 = 500$

Block Height	Transaction Description	Transaction Amount	Address Balance	Tainted Last (by all Outputs)	
				Tainted Funds Balance	Untainted Funds Balance
890000	Initial Balance	-	1,000	-	1,000
890001	Incoming Tainted Funds	2,000	3,000	2,000	1,000
890002	Outgoing Funds	-500	2,500	2,000	500
890003	Incoming Tainted Funds	1,000	3,500	3,000	500
890004	Outgoing Funds	-1,500	2,000	2,000	0
890005	Outgoing Funds	-1,000	1,000	1,000	0
890006	Incoming Clean Funds	3,000	4,000	1,000	3,000

Only once there are no untainted funds on the balance, tainted funds are taken out from the balance:
 $3,000 - (1,500 - 500)$

Figure 6. Example of Taint Last

23. Ultimately, the four additional methodologies—FIFO, LIFO, Pro Rata by Blocks, and Taint Last—are used as a means of verification. If BTC traced using the primary method do not appear when applying the other methodologies, the BTC and related accounts are eliminated from the findings. Coinfirm recognizes that in doing so, it is taking a very conservative approach that may and often does result in some of the BTC under investigation being excluded from Coinfirm's conclusions. Nonetheless, by taking a conservative approach, the conclusions that Coinfirm reaches in the course of its investigation can be easily defended in court if necessary.

24. Coinfirm's methods have been accepted by law enforcement agencies in various countries, including Switzerland. Had Ren challenged Coinfirm's investigations and methodologies at the time, Coinfirm might have disclosed additional portions of its investigative file and additional details regarding its methodology to the court so that the court could satisfy itself that the methodology utilized was sufficiently sound and reliable. Moreover, as I am no longer employed by Coinfirm, I am bound not to disclose any additional details of Coinfirm's highly confidential methodologies. Certainly, Mr. Cunha has not stated what he believes the

proper methodology is, and he has not disclosed any aspect of the methodology that he and TRM Labs employed when performing their own investigation.

25. Additionally, Mr. Cunha claims, without basis, that the timeframe Coinfirm chose for its analysis “does not make sense.” *See* Cunha Dec., ¶18. However, as can be seen in the chart in Figure 1 above, the time frame utilized was based upon when Mr. Vernon flooded ChipMixer with the Stolen Bitcoin, and when ChipMixer’s average daily BTC pool started to decline. Mr. Cunha is correct that there were a significant number of transfers of Stolen Bitcoin from ChipMixer closer in time to when Mr. Vernon flooded ChipMixer with Stolen Bitcoin. However, it is also apparent from Figure 1 that all of the Stolen Bitcoin was not withdrawn within the first month after Mr. Vernon transferred it to ChipMixer. I also disagree with Mr. Cunha’s suggestion that users had “strong incentives to withdraw from ChipMixer as soon as possible in order to prevent loss of the value deposited.” *See* Cunha Dec., ¶18. Considering Mr. Vernon’s purpose for utilizing ChipMixer, and the volume of the Stolen Bitcoin itself, it is apparent that Mr. Vernon was not concerned about withdrawing all of the Stolen Bitcoin from ChipMixer as quickly as possible to prevent the loss of value deposited. It is also not clear whether Mr. Vernon had the ability to withdraw all of the Stolen Bitcoin from ChipMixer in a mere few days following his initial deposits. Whatever Mr. Vernon’s motivation, it is apparent that he did not withdraw all of the Stolen Bitcoin by April 4, 2022. Likewise, ChipMixer’s BTC pool was still well above 2,000 when its systems were seized by German authorities.

26. In his Declaration, Mr. Cunha claims that I identified “a February 16, 2021 transfer of 1,080 BTC to the RenBridge wallet address 19iqYbeATe4RxghQZJnYVFU4mjUUu76EA6 as involving” Stolen Bitcoin. *See* Cunha Dec., ¶20. However, in the appendices to my December 27, 2022 Declaration, the earliest transaction involving that wallet address is April 27, 2021; between

April 27, 2021 and March 28, 2022, that wallet address received only 2.26423183 BTC of Stolen Bitcoin, and not the 1,080 BTC that Mr. Cunha suggests.

27. Mr. Cunha is also incorrect when he states that the wallet address 19iqYbeATe4RxghQZJnYVFU4mjUUu76EA6 is an address “to which users of the RenBridge service cannot make direct transfers.” *See* Cunha Dec., ¶20. Contrary to Mr. Cunha’s statement, anyone can make transfers to any existing blockchain address. While Mr. Cunha is correct that this particular wallet address is within a range that Ren used as administrative addresses, it appears that he misunderstands the reason why the address is included on Coinfirm’s tracking report. When a user wanted to deposit BTC with Ren, the user would have to request an address (the “Deposit Address”) from Ren. Once the Deposit Address was created, only the user and Ren would know that the Deposit Address existed on Ren’s system. Thus, as Stolen Bitcoin was deposited into Ren’s system, it would be deposited into one or more Deposit Addresses that were not immediately identifiable as existing on Ren’s system. However, Coinfirm’s real-time tracking would continue to track the Stolen Bitcoin from the Deposit Addresses and into Ren’s administrative address; such transfers occurred when the user’s BTC was moved from the Deposit Address into Ren’s administrative address.

28. Apparently conceding that Stolen Bitcoin went through ChipMixer and to RenBridge, Mr. Cunha speculates that “if Paul Vernon was attempting to obscure his transfers of BTC, it is likely that he quickly would have converted any renBTC to BTC and continued with additional obfuscating transfers.” *See* Cunha Dec., ¶23. However, Mr. Cunha cites no evidence to support this statement. I’m surprised that any experienced investigator would resort to such speculation without having any evidentiary basis for making the statement, and without presenting facts to substantiate such a statement.

29. Mr. Cunha also asserts that it is unlikely that any of the Stolen Bitcoin “remained with RenBridge as of April 2023 when it was transferred to cold storage.” *See* Cunha Dec., ¶22; *see also* ¶24 (“BTC that was originally transferred to RenBridge is almost certainly not the same BTC that was transferred to cold storage in April 2023”). However, Mr. Cunha has not presented any evidentiary basis for asserting that none of the Stolen Bitcoin was present when Ren transferred it to cold storage.² Since Ren was ordered to turn over the equivalent value of the 685 BTC, Coinfirm was not requested to confirm whether any of the Stolen Bitcoin remained in Ren’s possession at the time it transferred its BTC to cold storage.

30. Turning to Mr. Cunha’s criticism of Coinfirm’s tracking of Stolen Bitcoin to FTX, Mr. Cunha resorts to incorrect statements and what appears to be a statistical analysis of the transactions identified in the exhibit to my December 30, 2022 declaration. At the same time, it appears that Mr. Cunha intentionally ignores the details of the transactions themselves, perhaps because he realizes that the actual amounts that the accounts received from ChipMixer were significant.

31. Mr. Cunha claims that “of the 40 FTX addresses” in the Appendix to my December 30, 2022 Declaration, “only 5 (12%) have incoming transactions from ChipMixer.” *See* Cunha Dec., ¶27. While it is true that only 5 FTX addresses received funds *directly* from ChipMixer, what Mr. Cunha fails to mention is that only the amount received *directly* from ChipMixer by these 5 addresses totals 35.2617125 BTC, which is already greater than the amount of Stolen Bitcoin received by all the FTX addresses listed in my December 30, 2022 Declaration (34.59501771 BTC). The following tables summarizes Coinfirm’s findings with regard to accounts at FTX that

² Mr. Cunha also ignores the fact that when Ren transferred BTC to cold storage, it also effectively separated the BTC from the RenBridge information that would detail related transactions on other blockchain networks.

received funds directly from ChipMixer, including the total amount of BTC that the account received *directly* from ChipMixer.

FTX Address	Amount of Stolen Bitcoin Received	Total BTC Received Directly from ChipMixer
3LmNPNQRWt74qvVrsFZerUcSpkH4UZg5sA	6.94950202	31.1417357
3JhdmwrxYfTZ8EFQv639tQrLozs7eKeJxP	2.04799889	2.04799889
39ewULYNgyoCcgiddbnDGcMJ3UCeX92Ydv	1.99	2
35jAyRL5Bid9eaKvk2uifJBehJqSL48oNc	0.0319957	0.04298389
3luamNMQZkjGShvLz7AyZZpVKH5dcdzEbA	0.0159967	0.02899402
	TOTAL	35.2617125

Furthermore, Mr. Cunha gives the false impression that only direct transfers from ChipMixer should be counted: “Moreover, 10 (9%) of the mentioned transactions are deposits to FTX that are only indirectly sourced from ChipMixer after a considerable amount of intermediate transactions.” See Cunha Dec., ¶27. It is very common for bad actors to transfer digital assets from mixers to other private addresses prior to transferring the digital assets to addresses associated with known cryptocurrency services. If indirect blockchain transactions of fraudulent digital assets could not be considered fraudulent simply because the digital assets were transferred through other private (unhosted) intermediary wallets, it would render products from companies like TRM Labs virtually useless, since BTC sent through the simplest laundering scheme would have to be treated as clean BTC.

32. As an example, FTX address 32p1yFa54bJxwEnRiciCvQWLA4dWS7vzZr, identified in the Appendix to my December 30, 2022 Declaration, received zero (0) BTC directly from ChipMixer. However, this address indirectly received 0.70873244 Stolen Bitcoin and a total of 1.23020274 BTC from ChipMixer. Figure 7 below shows just some³ of the 1.23020274 BTC transfers from ChipMixer to this FTX address.

³ For simplicity, I present only a fragment of the full flow of BTC from ChipMixer to the FTX address in Figure 7.

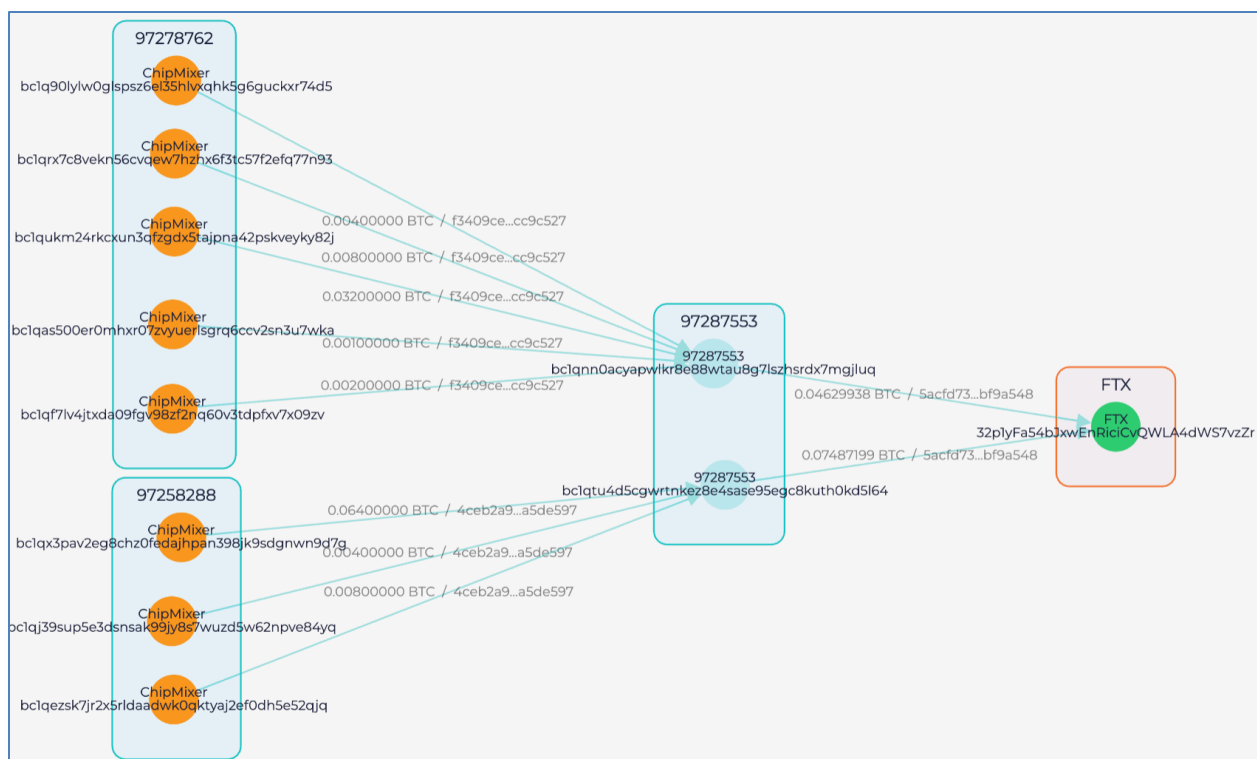


Figure 7 - Illustration of transactions traced from ChipMixer to an FTX address

In Figure 7, the orange nodes represent ChipMixer addresses, which sent BTC, including Stolen Bitcoin, to the blue nodes representing intermediate addresses (both owned by the same unknown individual). After this withdrawal from ChipMixer, the intermediate addresses deposited BTC to the FTX address represented by the green node. In addition to the Coinfirm analysis from my original declaration, I have confirmed these transfers in three other independent blockchain analysis tools. Mr. Cunha's claim that this address should be excluded from the analysis raises questions about his blockchain investigative skills.

33. Of the FTX addresses identified in the Appendix to my December 30, 2022 Declaration, four (4) of the FTX addresses received the majority of the Stolen Bitcoin identified. The following table summarizes Coinfirm's findings with regard to the majority of the 34 BTC of

Stolen Bitcoin that accounts at FTX received, including the total amount of BTC that the account received from ChipMixer in the same timeframe as the Stolen Bitcoin.⁴

FTX Address	Amount of Stolen Bitcoin Received	Total BTC Received from ChipMixer
3JjfbBQbdPrh7gW4kEhRAQQdoFkTdUpxLA	16.67896381	76.93
3LmNPNQRWt74qvVrsFZerUcSpkH4UZg5sA	6.94950202	72.27726128
3JhdmwrxYfTZ8EFQv639tQrLozs7eKeJxP	2.04799889	2.04799889
39ewULYNgyoCcgiddbnDGcMJ3UCeX92Ydv	1.99	2
TOTAL	27.66646472	153.2552602

34. Mr. Cunha also suggests that “the 34 BTC that [I] purported to trace to FTX was deposited into 39 distinct user accounts with no obvious connection to Paul Vernon, which further suggests that the 34 BTC does not constitute assets stolen from Cryptsy.” *See* Cunha Dec., ¶28. Mr. Cunha’s suggestion ignores two key points. First, the fact that accounts at FTX received portions of the Stolen Bitcoin—which were laundered via ChipMixer at a time when Mr. Vernon or someone working with Mr. Vernon who had access to the necessary keys flooded ChipMixer with a huge amount of Stolen Bitcoin—makes it impossible to state with any authority that Mr. Vernon is not associated with the accounts. At the very least, the transfers raise a question as to whether the accounts are in some way associated with Mr. Vernon. Second, it does not appear from Mr. Cunha’s Declaration that he made any effort to obtain the KYC information relating to the accounts that received portions of the Stolen Bitcoin. Either way, Mr. Cunha does not present

⁴ The percentages that Mr. Cunha includes in paragraph 27 of his Declaration are not helpful. To illustrate this point, consider the following two FTX addresses. Only forty percent (40%) of the transactions relating to FTX address 3JjfbBQbdPrh7gW4kEhRAQQdoFkTdUpxLA involved digital assets received from ChipMixer. While 40% may appear to be relatively low, the reality is that the account received 76.93 BTC from ChipMixer. At the current rate of \$60,300 for 1 BTC, the 40% represents \$4,638,879.00. In comparison, one hundred percent (100%) of the transactions relating to FTX address 3JhdmwrxYfTZ8EFQv639tQrLozs7eKeJxP involved digital assets received from ChipMixer, even though the FTX address received only 2.047 BTC (and 100% of the 2.047 BTC involved Stolen Bitcoin). At the current rate for BTC, that one hundred percent (100%) represents only \$123,434.10. Thus, focusing on the percentages does little to advance the analysis, and does not support the argument that Coinfirm’s investigation was in any way incorrect.

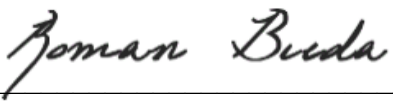
any factual basis for the assertion that the accounts receiving portions of Stolen Bitcoin have “no obvious connection with Paul Vernon.”

Improperly Attributed Statements

35. At numerous points throughout his Declaration, Mr. Cunha seemingly attributes the following statement to me: “some portion of the 685 BTC [were] transferred in April 2023 to cold storage wallets operated by the FTX Debtors.” *See* Cunha Dec., ¶¶ 5, 24, 25. However, neither my December 27, 2022 Declaration nor my December 30, 2022 Declaration include any such statement. I cannot conceive of an instance where I would reference transactions that had not yet occurred in a declaration, and the April 2023 transfer post-dates my 2022 Declarations.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 9th day of September, 2024.



Roman Bieda